



UNITED STATES PATENT AND TRADEMARK OFFICE

52
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073
26889	7590	04/18/2005	EXAMINER	
MICHAEL CHAN NCR CORPORATION 1700 SOUTH PATTERSON BLVD DAYTON, OH 45479-0001			PYZOGHA, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 04/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/651,979	Applicant(s) SHIELDS, ADRIAN	
	Examiner Michael Pyzocha	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 March 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 21-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 21-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

R

DETAILED ACTION

1. Claims 21-38 are pending.
2. Request for Continued Examination filed on 03/14/2005 has been received.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 21-23, 33-34 and 38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. The term "some" in claims 21, 33 and 38 is a relative term which renders the claim indefinite. The term "some" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of applying prior art the term "some" will be considered as "one or more".

Art Unit: 2137

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 21-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawan (US 20020062284) and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 21 and 33, Kawan discloses a portable computer, with non-secure user-accessible memory communicating (sending and receiving) with an external terminal (see paragraphs 22 and 32).

Kawan fails to disclose a) storing records of events experienced by the computer in memory within the computer; b) using some of the records as seed for generating plain text of a first session key K1; and then c) encrypting K1, transmitting K1 (encrypted), and encrypting the communications.

However, Menezes et al teaches storing records of events and using the records as a seed for generating a key (see page

Art Unit: 2137

172) and this key being a session key (see page 494) and encrypting the session key (see page 552).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's key generation to generate a session key, which is encrypted, to be transmitted in the portable computer of Kawan.

Motivation to do so would have been to generate a true random bit sequence for a key (see page 171), to limit available cipher text for cryptanalytic attacks (see page 494) and to protect the session key (see page 552).

As per claims 22, 24, 26-30, and 38, the modified Kawan and Menezes et al system further includes repeating the above mentioned steps to create a new session key for each new transaction (see page 494) and receiving encrypted messages encrypted by the session key (at both the portable computer and the external device) (see page 494 as applied to the communications of Kawan paragraph 32).

As per claims 23, 25, 31-32, and 34, the modified Kawan and Menezes et al system further includes the data used as the seed includes at least one element selected from the following group: recorded button selections, recorded pointer movements, recorded data entered by a user, current date setting, and current time setting (see page 172).

Art Unit: 2137

As per claims 35-37, the modified Kawan and Menezes et al system further includes the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN (see paragraph 30).

Conclusion

8. Examiner thanks Applicant for providing the pictorial of one mode of operation of the invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER